

1 **CLAIMS**

2 What is claimed is:

3 1. A method for use in curve-based cryptographic logic, the method
4 comprising:

5 determining at least one curve for use in cryptographically processing
6 selected information; and

7 determining pairings for use in cryptographically processing said selected
8 information by selectively using at least one parabola associated with said at least
9 one curve.

10
11 2. The method as recited in Claim 1, wherein said at least one curve
12 includes an elliptic curve.

13
14 3. The method as recited in Claim 1, wherein said pairings include
15 Weil pairings.

16
17 4. The method as recited in Claim 1, wherein said pairings include
18 Squared Weil pairings.

19
20 5. The method as recited in Claim 1, wherein said pairings include Tate
21 pairings.

22
23 6. The method as recited in Claim 1, wherein said pairings include
24 Squared Tate pairings.
25

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

7. The method as recited in Claim 1, further comprising:
cryptographically processing said selected information based on said pairings.

8. The method as recited in Claim 7, wherein cryptographically processing said selected information based on said pairings includes decrypting said selected information and outputting corresponding decrypted information.

9. The method as recited in Claim 7, wherein cryptographically processing said selected information based on said pairings includes encrypting said selected information and outputting corresponding encrypted information.

10. The method as recited in Claim 7, wherein cryptographically processing is configured to support at least one process selected from a group of processes comprising a key-based process, an identity-based encryption process, a product identification (ID)-based process, and a short signature-based process.

11. The method as recited in Claim 2, wherein determining said pairings for use in cryptographically processing said selected information further includes:

- determining at least a first function and a second function that are associated to certain multiples of a point on said elliptic curve;
- determining said parabola that is associated with said multiples of a point, and a line associated with said parabola;
- determining a third function based on said parabola and said line; and
- determining said pairings based on said third function.

12. The method as recited in Claim 11, wherein:

- said elliptic curve includes an elliptic curve E over a field K ;
- said first function and a second function include $f_{j,P}$ and $f_{k,P}$, respectively, for a point P on said elliptic curve E ;
- said parabola (parab) passes through points jP , jP , kP , $-2jP-kP$;
- said line is a vertical line through $-2jP-kP=(x_4,y_4)$ having equation equal to $x-x_4$
- said third function includes $f_{2j+k,P}$ such that

$$f_{2j+k,P}(X) = f_{j,P}(X) f_{k,P}(X) f_{j,P}(X) \frac{\text{parab}(X)}{(x(X) - x_4)}.$$

13. The method as recited in Claim 12, further comprising:

- evaluating said parabola for at least one point selected from points Q and $-Q$ on said elliptic curve E .

14. The method as recited in Claim 11, wherein:

said parabola (parab) has a form of

$$\text{parab}(\mathbf{X}) := (x(\mathbf{X}) - x_1)(x(\mathbf{X}) + x_1 + x_3 + a_2 + \lambda_1 \lambda_2) \\ + (\lambda_1 + \lambda_2 + a_1)(y_1 - y(\mathbf{X})); \text{ and}$$

said third function includes $f_{2j+k, \mathbf{P}}(\mathbf{X})$ such that

$$f_{2j+k, \mathbf{P}}(\mathbf{X}) = f_{j, \mathbf{P}}(\mathbf{X}) f_{k, \mathbf{P}}(\mathbf{X}) f_{j, \mathbf{P}}(\mathbf{X}) \frac{\text{parab}(\mathbf{X})}{(x(\mathbf{X}) - x_4)}.$$

15. The method as recited in Claim 14, further comprising:

evaluating said parabola for at least one point selected from points \mathbf{Q} and

$-\mathbf{Q}$ on said elliptic curve E .

16. The method as recited in Claim 11, wherein:

said parabola (parab) has a form of

$$\text{parab}(\mathbf{X}) := (x(\mathbf{X}) - x_2)(x(\mathbf{X}) + x_2 + x_3 + a_2 + \lambda_1 \lambda_2) \\ + (\lambda_1 + \lambda_2 + a_1)(y_2 - y(\mathbf{X}))$$

said third function includes $f_{2j+k, \mathbf{P}}(\mathbf{X})$ such that

$$f_{2j+k, \mathbf{P}}(\mathbf{X}) = f_{j, \mathbf{P}}(\mathbf{X}) f_{k, \mathbf{P}}(\mathbf{X}) f_{j, \mathbf{P}}(\mathbf{X}) \frac{\text{parab}(\mathbf{X})}{(x(\mathbf{X}) - x_4)}.$$

1 17. The method as recited in Claim 16, further comprising:
2 evaluating said parabola for at least one point selected from points Q and
3 $-Q$ on said elliptic curve E .

4
5 18. A computer-readable medium having computer-implementable
6 instructions for causing at least one processing unit to perform acts comprising:
7 determining at least one curve for use in cryptographically processing
8 selected information;
9 calculating pairings for use in cryptographically processing said selected
10 information by selectively using at least one parabola associated with said at least
11 one curve; and
12 cryptographically processing said selected information based on said
13 pairings.

14
15 19. The computer-readable medium as recited in Claim 18, wherein said
16 at least one curve includes an elliptic curve.

17
18 20. The computer-readable medium as recited in Claim 18, wherein said
19 pairings include at least one type of pairings selected from a group of different
20 pairings comprising Weil pairings, Squared Weil pairings, Tate pairings, and
21 Squared Tate pairings.

1 21. The computer-readable medium as recited in Claim 18, wherein
2 cryptographically processing said selected information based on said pairings
3 includes decrypting said selected information and outputting corresponding
4 decrypted information.

5
6 22. The computer-readable medium as recited in Claim 18, wherein
7 cryptographically processing said selected information based on said pairings
8 includes encrypting said selected information and outputting corresponding
9 encrypted information.

10
11 23. The computer-readable medium as recited in Claim 21, wherein
12 cryptographically processing is configured to support at least one process selected
13 from a group of processes comprising a key-based process, an identity-based
14 encryption process, a product identification (ID)-based process, and a short
15 signature-based process.

16
17 24. The computer-readable medium as recited in Claim 19, wherein
18 calculating said pairings further includes:

19 calculating at least a first function and a second function that are associated
20 to certain multiples of a point on said elliptic curve;

21 calculating said parabola that is associated with said multiples of a point,
22 and a line associated with said parabola;

23 calculating a third function based on said parabola and said line; and

24 calculating said pairings based on said third function.
25

25. The computer-readable medium as recited in Claim 24, wherein:
said elliptic curve includes an elliptic curve E over a field K ;
said first function and a second function include $f_{j,\mathbf{P}}$ and $f_{k,\mathbf{P}}$, respectively,
for a point \mathbf{P} on said elliptic curve E ;
said parabola (parab) passes through points $j\mathbf{P}$, $j\mathbf{P}$, $k\mathbf{P}$, $-2j\mathbf{P}-k\mathbf{P}$;
said line is a vertical line through
 $-2j\mathbf{P}-k\mathbf{P}=(x_4,y_4)$ having equation equal to $x-x_4$
said third function includes $f_{2j+k,\mathbf{P}}$ such that

$$f_{2j+k,\mathbf{P}}(\mathbf{X}) = f_{j,\mathbf{P}}(\mathbf{X}) f_{k,\mathbf{P}}(\mathbf{X}) f_{j,\mathbf{P}}(\mathbf{X}) \frac{\text{parab}(\mathbf{X})}{(x(\mathbf{X}) - x_4)}.$$

26. The computer-readable medium as recited in Claim 25, further
including:

evaluating said parabola for at least one point selected from points \mathbf{Q} and
 $-\mathbf{Q}$ on said elliptic curve E .

27. The computer-readable medium as recited in Claim 24, wherein:

said parabola (parab) has a form of

$$\begin{aligned} \text{parab}(\mathbf{X}) := & (x(\mathbf{X}) - x_1)(x(\mathbf{X}) + x_1 + x_3 + a_2 + \lambda_1 \lambda_2) \\ & + (\lambda_1 + \lambda_2 + a_1)(y_1 - y(\mathbf{X})); \text{ and} \end{aligned}$$

said third function includes $f_{2j+k,\mathbf{P}}$ such that

$$f_{2j+k,\mathbf{P}}(\mathbf{X}) = f_{j,\mathbf{P}}(\mathbf{X}) f_{k,\mathbf{P}}(\mathbf{X}) f_{j,\mathbf{P}}(\mathbf{X}) \frac{\text{parab}(\mathbf{X})}{(x(\mathbf{X}) - x_4)}.$$

28. The computer-readable medium as recited in Claim 27, further including:
evaluating said parabola for at least one point selected from points Q and $-Q$ on said elliptic curve E .

29. The computer-readable medium as recited in Claim 24, wherein:

said parabola (parab) has a form of

$$\text{parab}(\mathbf{X}) := (x(\mathbf{X}) - x_2)(x(\mathbf{X}) + x_2 + x_3 + a_2 + \lambda_1 \lambda_2) \\ + (\lambda_1 + \lambda_2 + a_1)(y_2 - y(\mathbf{X}))$$

said third function includes $f_{2j+k, P}(\mathbf{X})$ such that

$$f_{2j+k, P}(\mathbf{X}) = f_{j, P}(\mathbf{X}) f_{k, P}(\mathbf{X}) f_{j, P}(\mathbf{X}) \frac{\text{parab}(\mathbf{X})}{(x(\mathbf{X}) - x_4)}.$$

30. The computer-readable medium as recited in Claim 29, further including:
evaluating said parabola for at least one point selected from points Q and $-Q$ on said elliptic curve E .

1 31. An apparatus comprising:
2 memory configurable to store information; and
3 logic operatively coupled to said memory and configurable to at least
4 support cryptographic processing of selected information stored in said memory
5 by determining at least one curve for use in cryptographically processing selected
6 information and determining pairings for use in cryptographically processing said
7 selected information by selectively using at least one parabola associated with said
8 at least one curve.

9
10 32. The apparatus as recited in Claim 31, wherein said at least one curve
11 includes an elliptic curve.

12
13 33. The apparatus as recited in Claim 31, wherein said logic is further
14 configurable to perform said cryptographic processing of said selected
15 information.

16
17 34. The apparatus as recited in Claim 31, wherein said pairings include
18 at least one type of pairings selected from a group of different pairings comprising
19 Weil pairings, Squared Weil pairings, Tate pairings, and Squared Tate pairings.

20
21 35. The apparatus as recited in Claim 31, wherein said cryptographic
22 processing of said selected information includes decrypting said selected
23 information and outputting corresponding decrypted information.

1 36. The apparatus as recited in Claim 31, wherein said cryptographic
2 processing of said selected information includes encrypting said selected
3 information and outputting corresponding encrypted information.

4
5 37. The apparatus as recited in Claim 35, wherein said cryptographic
6 processing at least supports at least one process selected from a group of processes
7 comprising a key-based process, an identity-based encryption process, a product
8 identification (ID)-based process, and a short signature-based process.

9
10 38. The apparatus as recited in Claim 32, wherein said logic is further
11 configured to calculate at least a first function and a second function that are
12 associated to certain multiples of a point on said elliptic curve, calculate said
13 parabola that is associated with said multiples of a point, and a line associated with
14 said parabola, calculate a third function based on said parabola and said line, and
15 calculate said pairings based on said third function.

39. The apparatus as recited in Claim 38, wherein:
said elliptic curve includes an elliptic curve E over a field K ;
said first function and a second function include $f_{j,\mathbf{P}}$ and $f_{k,\mathbf{P}}$, respectively,
for a point \mathbf{P} on said elliptic curve E ;
said parabola (parab) passes through points $j\mathbf{P}$, $j\mathbf{P}$, $k\mathbf{P}$, $-2j\mathbf{P}-k\mathbf{P}$;
said line is a vertical line through
 $-2j\mathbf{P}-k\mathbf{P}=(x_4,y_4)$ having equation equal to $x-x_4$
said third function includes $f_{2j+k,\mathbf{P}}$ such that

$$f_{2j+k,\mathbf{P}}(\mathbf{X}) = f_{j,\mathbf{P}}(\mathbf{X}) f_{k,\mathbf{P}}(\mathbf{X}) f_{j,\mathbf{P}}(\mathbf{X}) \frac{\text{parab}(\mathbf{X})}{(x(\mathbf{X}) - x_4)}.$$

40. The apparatus as recited in Claim 39, wherein said logic is further
configured to evaluate said parabola for at least one point selected from points \mathbf{Q}
and $-\mathbf{Q}$ on said elliptic curve E .

41. The apparatus as recited in Claim 38, wherein:

said parabola (parab) has a form of

$$\begin{aligned} \text{parab}(\mathbf{X}) := & (x(\mathbf{X}) - x_1)(x(\mathbf{X}) + x_1 + x_3 + a_2 + \lambda_1 \lambda_2) \\ & + (\lambda_1 + \lambda_2 + a_1)(y_1 - y(\mathbf{X})); \text{ and} \end{aligned}$$

said third function includes $f_{2j+k,\mathbf{P}}(\mathbf{X})$ such that

$$f_{2j+k,\mathbf{P}}(\mathbf{X}) = f_{j,\mathbf{P}}(\mathbf{X}) f_{k,\mathbf{P}}(\mathbf{X}) f_{j,\mathbf{P}}(\mathbf{X}) \frac{\text{parab}(\mathbf{X})}{(x(\mathbf{X}) - x_4)}.$$

42. The apparatus as recited in Claim 41, wherein said logic is further configured to evaluate said parabola for at least one point selected from points \mathbf{Q} and $-\mathbf{Q}$ on said elliptic curve E .

43. The apparatus as recited in Claim 38, wherein:

said parabola (parab) has a form of

$$\begin{aligned} \text{parab}(\mathbf{X}) := & (x(\mathbf{X}) - x_2)(x(\mathbf{X}) + x_2 + x_3 + a_2 + \lambda_1 \lambda_2) \\ & + (\lambda_1 + \lambda_2 + a_1)(y_2 - y(\mathbf{X})) \end{aligned}$$

said third function includes $f_{2j+k, \mathbf{P}}(\mathbf{X})$ such that

$$f_{2j+k, \mathbf{P}}(\mathbf{X}) = f_{j, \mathbf{P}}(\mathbf{X}) f_{k, \mathbf{P}}(\mathbf{X}) f_{j, \mathbf{P}}(\mathbf{X}) \frac{\text{parab}(\mathbf{X})}{(x(\mathbf{X}) - x_4)}.$$

44. The apparatus as recited in Claim 43, wherein said logic is further configured to evaluate said parabola for at least one point selected from points \mathbf{Q} and $-\mathbf{Q}$ on said elliptic curve E .